43 : 1st half.10-AM(k)

Con. 3495-10.　　　　　　　　(REVISED COURSE)　　　　　　　　AN–4588

(3 Hours)　　　　　　　　　　　　[Total Marks : 100

N.B.:　(1)　Question No. **1** is **compulsory**.
　　　　(2)　Attempt any **four** questions out of remaining **six** questions.

1.　(a)　What are the key principles of security ? Explain with example ?　　5
　　(b)　Compare secret key and public key encryption ?　　5
　　(c)　Distinguish among Vulnerability, threat and control.　　5
　　(d)　List three controls that could be applied to detect or prevent salami attacks ?　　5

2.　(a)　Compare AES and DES. Comment on Double and Triple DES ?　　10
　　(b)　What is Digital signature ? Explain in brief ?　　10

3.　(a)　Explain Denial of Service attack in networks.　　10
　　(b)　List and explain various malicious and non-malicious codes with examples.　　10

4.　(a)　What is Firewall ? Describe the types of firewalls with their limitations ?　　10
　　(b)　Describe the types of IDSs and their limitations ? Why we need hybrid IDSs ?　　10

5.　(a)　Explain the use of temporal, physical and logical separation for security in Computing environment ?　　10
　　(b)　What are the various forms of protection that operating system applies at the file level.　　10

6.　(a)　What is the term Risk Analysis ? Explain in detail the steps in Risk analysis ?　　10
　　(b)　Explain Secure-Email system with example.　　10

7.　Write short notes on any **three** of the following :—　　20
　　(a)　Kerberos System
　　(b)　RSA Algorithm
　　(c)　Hash functions
　　(d)　ARP Spoofing.